

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-289299  
(43)Date of publication of application : 10.10.2003

(51)Int.Cl. H04L 9/14  
G09C 1/00  
H04L 9/08  
H04L 9/32  
H04L 12/66

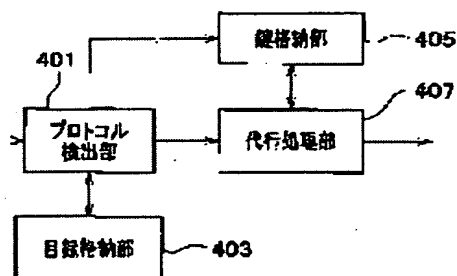
(21)Application number : 2002-378796 (71)Applicant : SAMSUNG ELECTRONICS CO LTD  
(22)Date of filing : 27.12.2002 (72)Inventor : PARK SANG-DO

(30)Priority  
Priority number : 2002 200200514 Priority date : 04.01.2002 Priority country : KR

## (54) COMMUNICATION CONNECTING APPARATUS FOR EXECUTING FUNCTION OF SECURITY PROTOCOL, AND COMMUNICATION CONNECTING METHOD THEREOF

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a communication connecting apparatus for executing a function of a security protocol, and a communication connecting method thereof.  
**SOLUTION:** This communication connecting apparatus comprises a protocol detecting unit 401 for detecting a key exchange protocol in a packet received from an external device, a list storage unit for storing a list of devices for executing a certification procedure between devices for transmitting/receiving data, and an agent unit for executing a certification procedure by transmitting a certification signal to the external device, when a device corresponding to the key exchange unit exists in the device list. Also, the apparatus may comprise a key storage unit 405 for storing a session key for forming a communication path between the internal and external devices. In this way, the apparatus can execute the security protocol function on behalf of a home device having insufficient processing performance of security protocol.



## LEGAL STATUS

[Date of request for examination] 27.12.2002  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-289299

(P2003-289299A)

(43) 公開日 平成15年10月10日 (2003. 10. 10)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-コ-ト*(参考)
H 0 4 L 9/14		G 0 9 C 1/00	6 4 0 E 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 12/66	B 5 K 0 3 0
H 0 4 L 9/08		9/00	6 4 1
9/32			6 0 1 C
12/66			6 0 1 E
審査請求 有 請求項の数 8 O L (全 7 頁) 最終頁に続く			

(21) 出願番号 特願2002-378796(P2002-378796)

(22) 出願日 平成14年12月27日 (2002. 12. 27)

(31) 優先権主張番号 2 0 0 2 - 0 0 5 1 4

(32) 優先日 平成14年1月4日 (2002. 1. 4)

(33) 優先権主張国 韓国 (K R)

(71) 出願人 390019839

三星電子株式会社

大韓民国京畿道水原市八達区梅灘洞416

(72) 発明者 朴 相 度

大韓民国 ソウル特別市 江南区 三成2

洞 曙光アパート 102棟 807号

(74) 代理人 100064414

弁理士 磯野 道造

Fターム(参考) 5J104 AA07 EA04 EA15 KA02 KA05

NA03 PA07

5K030 GA15 HA08 HC01 HD03 KA06

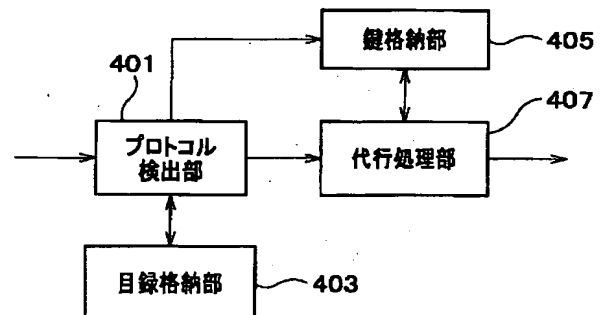
LC13

(54) 【発明の名称】 セキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法

(57) 【要約】

【課題】 セキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法を提供する。

【解決手段】 本発明に係る通信連結装置は、外部のデバイスから送信されたパケットに対し鍵交換プロトコルを検出するプロトコル検出部401と、データを送受信する機器相互間の認証手続を代行するためのデバイスの目録が格納された目録格納部403と、前記鍵交換プロトコルに対応する内部のデバイスが前記目録にあると、前記外部のデバイスに認証信号を送信して前記認証手続を実行する代行処理部407とを含んで構成される。更に、前記内部のデバイスと前記外部のデバイスとの間の通信経路を形成するためのセッション鍵を格納する鍵格納部405を含んで構成してもよい。これにより、本発明に係る通信連結装置は、セキュリティプロトコルの処理能力が不足しているホームデバイスのために、セキュリティプロトコル機能を代行することができる。



## 【特許請求の範囲】

【請求項1】 外部のデバイスから送信されたバケットに対し鍵交換プロトコルを検出するプロトコル検出部と；データを送受信する機器相互間の認証手続を代行するためのデバイスの目録が格納された目録格納部と；前記鍵交換プロトコルに対応する内部のデバイスが前記目録にあると、前記外部のデバイスに認証信号を送信して前記認証手続を実行する代行処理部と；を含んで構成されることを特徴とするセキュリティプロトコルの機能を実行する通信連結装置。

【請求項2】 前記内部のデバイスと前記外部のデバイスとの間の通信経路を形成するためのセッション鍵（Session key）を格納する鍵格納部を、更に含み、前記代行処理部は、前記鍵交換プロトコルに対応する前記セッション鍵を取得して前記内部のデバイスに転送することにより、前記内部のデバイスと前記外部のデバイスとの通信経路を連結することを特徴とする請求項1に記載のセキュリティプロトコルの機能を実行する通信連結装置。

【請求項3】 前記鍵格納部は、前記内部のデバイスに提供された個人鍵（private key）を、更に格納し、前記代行処理部は、前記鍵交換プロトコルに対応する前記個人鍵を取得して前記外部のデバイスへ転送し、前記外部のデバイスは、受信した前記個人鍵によって前記内部のデバイスを確認することを特徴とする請求項2に記載のセキュリティプロトコルの機能を実行する通信連結装置。

【請求項4】 前記鍵格納部は、前記内部のデバイスに提供された公開鍵（public key）を格納し、前記代行処理部は、前記鍵交換プロトコルに対応する前記内部のデバイスが前記目録にないとは判定した場合に、前記公開鍵を前記外部のデバイスへ転送し、前記外部のデバイスは、受信した前記公開鍵によって前記内部のデバイスを認識することを特徴とする請求項2に記載のセキュリティプロトコルの機能を実行する通信連結装置。

【請求項5】 外部のデバイスから送信されたバケットに対し鍵交換プロトコルを検出する段階と；前記検出された鍵交換プロトコルに基づいて認証手続を実行する内部のデバイスの目録を検索する段階と；前記鍵交換プロトコルに対応する前記内部のデバイスが目録格納部にあると判定した場合に、前記外部のデバイスへ認証信号を送信して前記認証手続を実行する段階と；を含んで構成されることを特徴とするセキュリティプロトコルの機能を実行する通信連結方法。

【請求項6】 前記内部のデバイスと前記外部のデバイスとの間の通信経路を形成するための少なくとも1つのセッション鍵を生成する段階と；前記鍵交換プロトコル

に対応する少なくとも1つの前記セッション鍵を取得し、少なくとも1つの前記セッション鍵のうち1つを前記内部のデバイスへ転送する段階と；を更に含んで構成され、

前記外部のデバイスに連結される前記内部のデバイスは、受信した前記セッション鍵によって前記通信経路が形成されることを特徴とする請求項5に記載のセキュリティプロトコルの機能を実行する通信連結方法。

【請求項7】 少なくとも1つの固有の個人鍵を生成する段階と；前記少なくとも1つの固有の個人鍵のうち、前記鍵交換プロトコルに対応する前記個人鍵を取得して前記外部のデバイスへ転送する段階と；を更に含んで構成され、

前記外部のデバイスは、受信した前記個人鍵によって前記内部のデバイスを確認することを特徴とする請求項6に記載のセキュリティプロトコルの機能を実行する通信連結方法。

【請求項8】 少なくとも1つの公開鍵を生成する段階と；前記鍵交換プロトコルに対応する前記内部のデバイスが前記目録にないとは判定した場合に、少なくとも1つの前記公開鍵のうち1つを前記外部のデバイスへ転送する段階と；を更に含み、

前記外部のデバイスは、受信した前記公開鍵によって前記内部のデバイスを認識することを特徴とする請求項6に記載のセキュリティプロトコルの機能を実行する通信連結方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、セキュリティプロトコル機能を実行する通信連結装置及びその通信連結方法に関し、より詳細には、セキュリティプロトコルの処理能力が不足しているホームデバイスのために、セキュリティプロトコル機能を代行するホームゲートウェイシステム、及びその実行方法に関する。

## 【0002】

【従来の技術】一般に、ゲートウェイシステムとは、相互に異なるデータ通信プロトコルを使用する通信ネットワークの間に位置し、相互に異なるプロトコルを使用する通信ネットワークの間で転送されるデータを、各通信ネットワークに対応したデータに変換する機能を実行するシステムをいう。

【0003】特に、ホームゲートウェイは、インターネット又は広域サービスネットワーク（外部ネットワーク）とホームネットワークの間に位置し、両者間で転送されるデータを各通信ネットワークに対応したデータに変換する機能を実行するものである。従って、ホームゲートウェイは、連結された外部ネットワークとホームネットワークとが相互に円滑に適応できるように、各通信ネットワークに対して独立性を有している必要がある。

【0004】ホームゲートウェイは、外部ネットワーク

の端末機として機能するAGM (Access Gateway Module) と、ホームネットワークの端末機として機能するPNM (Premise Network Module) と、PNMその他の内部装置とAGMとの間のインターフェイスとして機能するIDI (Internal Digital Interface) と、全体のシステムを管理するオペレーティングシステム、及びその他の機能を実行するSM (Service Module) などで構成される。

【0005】図1は、従来の一般的なネットワークの構成を模式的に示す図である。図1に示すように、ローカルデバイス10は、ホームネットワーク20を通して相互に連結されている。ホームネットワーク20は、ホームゲートウェイ30を通してインターネット40に接続されている。また、遠隔のクライアント50は、インターネット40を通してホームゲートウェイ30に接続されている。

【0006】ここで、ローカルデバイス10は、ホームネットワーク20に連結された、デジタルテレビ、ファクシミリ、及びコンピュータ等の情報端末機と称される情報機器を指す。また、遠隔のクライアント50は、インターネット40に連結されたコンピュータ、携帯電話機等の遠隔の端末機を指す。このような構成によって、遠隔のクライアント50は、遠隔地においてもホームネットワーク20に接続されたローカルデバイス10とデータを送受信することができる。

【0007】一般に、ホームネットワーク20に連結されたローカルデバイス10が、外部ネットワーク40の遠隔のクライアント50とセキュアチャンネル (Secure Channel) を設定する方法としては2つの方法がある。

【0008】第1の方法は、図2に示すように、遠隔のクライアント50とホームゲートウェイ30との間に、セキュアトンネルを設ける方法である。

【0009】図2を参照すると、ダミーデバイス11は、ホームネットワーク20に連結されており、ホームネットワーク20は、ホームゲートウェイ30を通してインターネット40に接続されている。さらに、インターネット40には、公認IP (Internet Protocol) アドレスをインターネット40に付与する、ISP (Internet Service Provider) 43が接続されている。また、ホームゲートウェイ30と遠隔のクライアント50は、セキュアトンネル55を通して連結されている。ここで、ダミーデバイス11とは、ホームネットワーク20に連結されているデバイスのうち、セキュリティプロトコルを有しないデバイスを指す。

【0010】ホームゲートウェイ30にはISP43から公認IPアドレスが提供されて、遠隔のクライアント50はISP43からホームゲートウェイ30に提供さ

れる公認IPアドレスによって、ホームゲートウェイ30の位置を把握する。

【0011】ホームゲートウェイ30と遠隔のクライアント50は、ホームゲートウェイ30と遠隔のクライアント50との間に設定されたセキュアトンネルを介して相互にデータを通信する。また、ホームゲートウェイ30は、ホームネットワーク20に連結されたダミーデバイス11に個人IPを付与し、付与された個人IPアドレスによって各ダミーデバイス11を認識してデータを送受信する。

【0012】これにより、遠隔のクライアント50は、公認IPアドレスによってホームゲートウェイ30を認識してデータを通信し、ホームゲートウェイ30は、個人IPアドレスによってホームネットワーク20に連結されたダミーデバイス11を認識してデータを通信することができる。

【0013】しかし、前記の方法においては、ホームゲートウェイ30と遠隔のクライアント50との間に設定されたセキュアトンネルを介することで、ホームゲートウェイ30と遠隔のクライアント50との間のセキュリティは保証されるが、ホームゲートウェイ30とダミーデバイス11との間のホームネットワーク20の内部におけるセキュリティは保証されないという問題点がある。

【0014】ホームネットワーク20に連結されたローカルデバイス10が、外部網の遠隔のクライアント50とセキュアチャンネルを設定するための第2の方法は、図3に示すように、ホームデバイス10が遠隔のクライアント50と1対1に契約 (Security Association; SA) を結ぶ方法である。

【0015】図3を参照すると、ホームネットワーク20に連結された各デバイス13は、インターネット40に連結されたISP43から公認IPアドレスが付与される。ここでのデバイス13は、それぞれ公認IPが付与された情報機器のことをいう。

【0016】遠隔のクライアント50は、インターネット40を通してホームゲートウェイ30に連結され、各デバイス13は、ホームゲートウェイ30を通してインターネット40に連結される。遠隔のクライアント50は、各デバイス13に付与された公認IPアドレスによって、ホームネットワーク20に連結されたデバイス13を認識してデータを送受信する。

【0017】しかし、前記第2の方法によれば、ホームネットワーク20と遠隔のクライアント50の間だけでなくホームネットワークの内部におけるセキュリティも保証されるが、ホームネットワーク20に連結された各デバイス13が全てセキュリティプロトコルを有しなければならぬため、設置費用が高くなるという問題点がある。

【0018】

10

20

30

40

50

【発明が解決しようとする課題】本発明は、前記したような問題点を解決するために、ホームネットワークに連結された各デバイスが外部の遠隔のクライアントに連結される際に、ホームネットワークの内部、及び外部におけるセキュリティが保証され得ると共に、設置費用も安くできる通信連結装置及びその連結方法を提供することを目的とする。

【0019】

【課題を解決するための手段】前記目的を達成するための本発明に係るセキュリティプロトコルの機能を実行する通信連結装置は、外部のデバイスから送信されたパケットに対して鍵交換プロトコルを検出するプロトコル検出部と、データを送受信する機器相互間の認証手続を代行するためのデバイスの目録が格納された目録格納部と、前記鍵交換プロトコルに対応する内部のデバイスが前記目録にあると、前記外部のデバイスに認証信号を送信して前記認証手続を実行する代行処理部とを含んで構成される（請求項1）。

【0020】前記通信連結装置において、望ましくは、内部のデバイスと外部のデバイスとの間の通信経路を形成するためのセッション鍵（Session key）を格納する鍵格納部を、更に含み、代行処理部は、鍵交換プロトコルに対応する前記セッション鍵を取得して前記内部のデバイスに転送することにより、前記内部のデバイスと前記外部のデバイスとの通信経路を連結するように構成される（請求項2）。

【0021】また、前記通信連結装置において、望ましくは、鍵格納部は、内部のデバイスに提供された個人鍵（private key）を、更に格納し、代行処理部は、鍵交換プロトコルに対応する個人鍵を取得して外部のデバイスへ転送し、外部のデバイスは、受信した個人鍵によって前記内部のデバイスを確認するように構成する（請求項3）。

【0022】前記通信連結装置において、より望ましくは、鍵格納部は、内部のデバイスに提供された公開鍵（public key）を格納し、代行処理部は、鍵交換プロトコルに対応する内部のデバイスが目録にないと判定した場合に、公開鍵を前記外部のデバイスへ転送し、外部のデバイスは、受信した公開鍵によって内部のデバイスを認識するように構成する（請求項4）。

【0023】一方、前記目的を達成するための本発明に係るセキュリティプロトコルの機能を実行する通信連結方法は、外部のデバイスから送信されたパケットに対し鍵交換プロトコルを検出する段階と、前記検出された鍵交換プロトコルに基づいて認証手続を実行する内部のデバイスの目録を検索する段階と、前記鍵交換プロトコルに対応する前記内部のデバイスが目録格納部にあると判定した場合に、前記外部のデバイスへ認証信号を送信して前記認証手続を実行する段階とを含んで構成される（請求項5）。

【0024】前記通信連結方法において、望ましくは、内部のデバイスと外部のデバイスとの間の通信経路を形成するための少なくとも1つのセッション鍵を生成する段階と、鍵交換プロトコルに対応する少なくとも1つのセッション鍵を取得して、少なくとも1つのセッション鍵のうち1つを内部のデバイスへ転送する段階とを更に含んで構成され、外部のデバイスに連結される内部のデバイスは、受信したセッション鍵によって通信経路が形成される（請求項6）。

【0025】また、前記通信連結方法において、望ましくは、少なくとも1つの固有の個人鍵を生成する段階と、少なくとも1つの固有の個人鍵のうち、鍵交換プロトコルに対応する個人鍵を取得して外部のデバイスへ転送する段階とを更に含んで構成され、外部のデバイスは、受信した個人鍵によって内部のデバイスを確認するように構成する（請求項7）。

【0026】さらに、前記通信連結方法において、少なくとも1つの公開鍵を生成する段階及び鍵交換プロトコルに対応する内部のデバイスが目録にないと判定した場合に、少なくとも1つの公開鍵のうち1つを外部のデバイスへ転送する段階とを更に含み、外部のデバイスは、受信した公開鍵によって内部のデバイスを認識するように構成する（請求項8）。

【0027】

【発明の実施の形態】以下、図面に基づいて、本発明をより詳細に説明する。図4は、本発明に係るネットワークの構成を模式的に示す図である。図4に示すように、デバイス13及びダミーデバイス15は、ホームネットワークに連結されており、ホームネットワーク20はホームゲートウェイ30に接続されている。ホームゲートウェイ30はインターネット40に連結されており、インターネット40にはISP43及び遠隔のクライアント50が連結されている。ここで、図1から図3に示されている各部分と同一の構成を有する部分に対しては同一の参照符号を付してある。

【0028】デバイス13は、ホームネットワーク20に連結される情報機器のなかで、セキュリティプロトコルが搭載された情報機器を指し、ダミーデバイス15は、ホームネットワーク20に連結される情報機器のうちセキュリティプロトコルが搭載されていないデバイスを指す。

【0029】ホームゲートウェイ30には、ISP43から公認IPアドレスが提供され、遠隔のクライアント50は、このISP43からホームゲートウェイ30に提供された公認IPアドレスによって、ホームゲートウェイ30の位置を把握するようになっている。

【0030】図5は、本発明に係る通信連結装置の構成を模式的に示すブロック図である。図5に示すように、本発明に係る通信連結装置、すなわちホームゲートウェイ30は、プロトコル検出部401、目録格納部40

3、鍵格納部405、及び代行処理部407とを備えて構成されている。

【0031】プロトコル検出部401は、外部のデバイス、すなわち遠隔のクライアント50から受信したパケットに対して、鍵交換プロトコルを検出する。目録格納部403は、データを送受信する機器相互間の認証手続を代行するためのデバイス、すなわちダミーデバイス15の目録を格納する。鍵格納部405は、ダミーデバイス15と遠隔のクライアント50との間の通信経路を形成するためのセッション鍵、及びデバイス13に付与された個人鍵及び公開鍵を格納する。

【0032】代行処理部407は、検出された鍵交換プロトコルに対応するダミーデバイス15の目録が目録格納部403にあると、遠隔のクライアント50に認証信号を送信して認証手続を代行するものである。また、代行処理部407は、検出された鍵交換プロトコルに対応するセッション鍵を取得してデバイス13及びダミーデバイス15の両方またはいずれか一方に転送し、デバイス13及びダミーデバイス15の両方またはいずれか一方と遠隔のクライアント50との間に通信経路を形成する。

【0033】さらに、代行処理部407は、鍵交換プロトコルに対応する個人鍵を取得して遠隔のクライアント50に転送し、遠隔のクライアント50は、受信した個人鍵によってデバイス13及びダミーデバイス15の両方またはいずれか一方を確認する。一方、代行処理部407は、鍵交換プロトコルに対応するダミーデバイス15の目録が目録格納部403にない場合は、公開鍵を遠隔のクライアント50に転送し、遠隔のクライアント50は受信した公開鍵によってホームネットワークに連結されたデバイス13を認識する。

【0034】図6は、図5に示す本発明に係る通信連結装置の通信連結方法を示すフローチャートである。図6示すように、ホームゲートウェイ30のプロトコル検出部401は、遠隔のクライアント50からパケットを受信すると、この受信したパケットから鍵交換プロトコルを検出する(ステップS501)。また、プロトコル検出部401は、この検出された鍵交換プロトコルに対応するデバイス13及びダミーデバイス15の両方またはいずれか一方、すなわちパケットが転送しようとする目的デバイスと遠隔のクライアント50との間の通信経路を形成するためのセッション鍵を生成する(ステップS503)。

【0035】プロトコル検出部401は、生成されたセッション鍵を鍵格納部405に格納する(ステップS505)。また、プロトコル検出部401は、代行処理部407へセッション鍵の生成及び格納を知らせる信号を転送する。

【0036】代行処理部407は、鍵格納部405から鍵交換プロトコルに対応するセッション鍵を取得し、こ

のように取得したセッション鍵に対応するデバイス13及びダミーデバイス15の両方またはいずれか一方に転送する(ステップS507)。ここで、代行処理部407は、鍵格納部405からセッション鍵を取得することにより具現したが、プロトコル検出部401から生成されたセッション鍵を直接受信してデバイス13及びダミーデバイス15の両方またはいずれか一方に転送するようにも具現できる。これにより、セッション鍵を受信したデバイス13及びダミーデバイス15の両方またはいずれか一方と遠隔のクライアント50との間に通信経路が形成される。

【0037】次に、プロトコル検出部401は、目録格納部403を検索し(ステップS509)、検出された鍵交換プロトコルに対応するデバイス、すなわち、ダミーデバイス15の目録があるか否かを判断する(ステップS511)。

【0038】目録格納部403に、鍵交換プロトコルに対応するダミーデバイス15の目録があると、プロトコル検出部401は、ダミーデバイス15に与えるための固有の個人鍵を生成する(ステップS513)。プロトコル検出部401は、生成された個人鍵を鍵格納部405に格納する(ステップS515)。

【0039】プロトコル検出部401は、遠隔のクライアント50と通信経路が形成されたダミーデバイスからデータを受信すると、受信されたデータを代行処理部407に転送する。代行処理部407は、プロトコル検出部401から転送されたデータを受信し、鍵格納部405を検索してデータを送り出したダミーデバイス15に対応する個人鍵を取得する。このようにして取得された個人鍵は、受信したデータと共に代行処理部407によって遠隔のクライアント50に転送される(ステップS517)。遠隔のクライアント50は、受信した個人鍵によってダミーデバイス15を確認する。

【0040】一方、目録格納部403に鍵交換プロトコルに対応するダミーデバイス15の目録がない場合は、プロトコル検出部401は、代行処理部407に目録の不在信号を転送する。代行処理部407は、プロトコル検出部401から目録不在信号を受信すると、鍵格納部405からデバイス13に与えられた公開鍵を検索する(ステップS519)。

【0041】ここで、デバイス13は、ホームネットワーク20に連結された情報機器のうち、セキュリティプロトコルが搭載された情報機器であり、ISP43から公認IPアドレスが付与されている。デバイス13に付与された公認IPアドレスは鍵格納部405に格納されている。

【0042】デバイス13からデータを受信したとき、代行処理部407は、鍵格納部405から鍵交換プロトコルに対応する公開鍵を取得して、遠隔のクライアント50に転送する(ステップS521)。遠隔のクライ

10

20

30

40

50

ント50は、代行処理部407から受信した公開鍵によって、ホームネットワーク20に連結されたデバイス13を認識する。

【0043】これにより、ホームゲートウェイ30は、ホームネットワーク20に連結されたデバイス13及びダミーデバイス15の両方またはいずれか一方と遠隔のクライアント50との間に通信経路を形成する場合において、ホームネットワーク20の外部のみならず、内部におけるセキュリティも保証され得る。

【0044】本発明は、前記したような特定の望ましい実施形態のみに限定されるものではなく、本発明の技術的思想に基づく限りにおいて、当該発明の属する技術分野で通常の知識を有する者であれば何人であっても、各種の多様な実施形態を具現することが可能であることは勿論のこと、このような各種の多様な実施形態は、本明細書に記載された特許請求の範囲内にある。

【0045】

【発明の効果】以上の通りに構成された本発明によれば、以下の効果を奏する。すなわち、本発明に係るセキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法によれば、セキュリティプロトコルの処理能力が不足しているホームデバイスのために、セキュリティプロトコル機能を代行することができる。更に、ホームネットワークに連結されたデバイス及び遠隔のクライアントの間でデータを送受信する際に、ホームネットワークの内部のみならず外部におけるセキュリティが保証され得ると共に、設置費用を低減することがで

\*きる。

【図面の簡単な説明】

【図1】従来の一般的なネットワークの構成を模式的に示す図である。

【図2】ホームゲートウェイと遠隔のクライアントとの間にセキュアトンネルが設置されたネットワークの構成を模式的に示す図である。

【図3】ホームネットワークに連結された各デバイスと遠隔のクライアントとの間にセキュリティ関係が形成されたときのネットワークの構成を模式的に示す図である。

【図4】本発明に係るセキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法におけるネットワークの構成を模式的に示す図である。

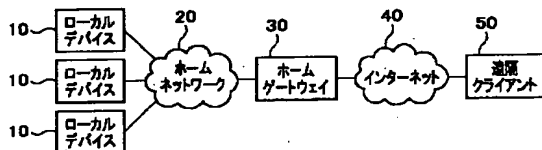
【図5】本発明に係る通信連結装置を模式的に示すブロック図である。

【図6】図5の装置による通信連結方法を示すフローチャートである。

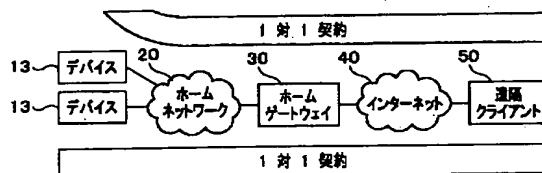
【符号の説明】

- 10 ローカルデバイス
- 11、15 ダミーデバイス
- 13 デバイス
- 20 ホームネットワーク
- 30 ホームゲートウェイ
- 40 インターネット
- 50 遠隔のクライアント

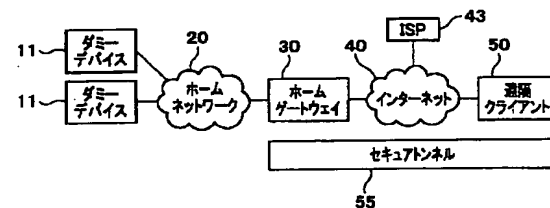
【図1】



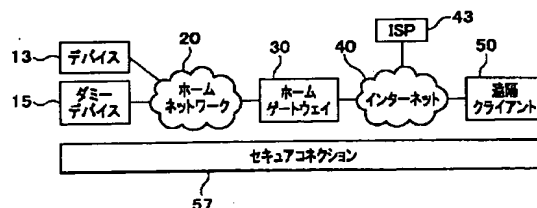
【図3】



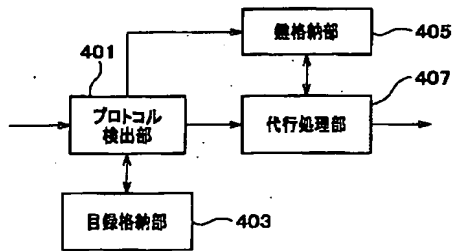
【図2】



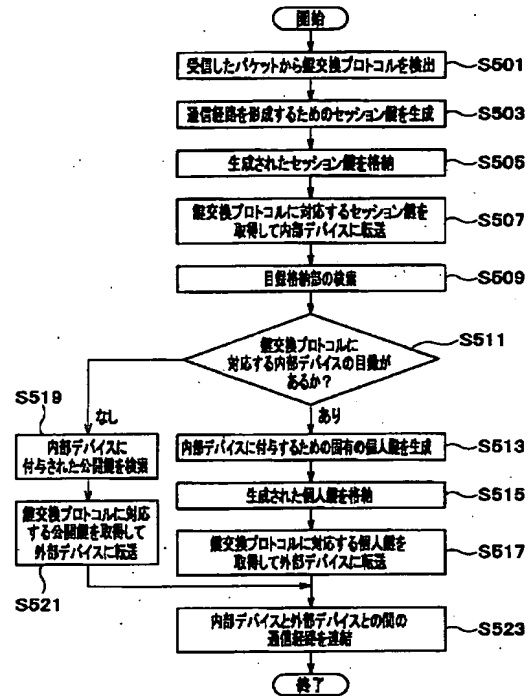
【図4】



【図5】



【図6】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I  
H 0 4 L 9/00

テーマコード (参考)

6 7 5 B  
6 0 1 B